ENDPOINT PROTECTION PROJECT 2014

Presentation to CTSC

UNIVERSITY OF WATERLOO

QUICK TOUR

- Why do we need protection at all?
- What forms might those protections take?
- The project that started this
- Questions for you to consider

MALWARE ATTACK VECTORS

- Email
  - » Document attachments
  - » Malicious URLs
- Websites
- USB Sticks
- Other network attacks

ANTIVIRUS EFFECTIVENESS

- 2012 Study at University of Alabama at Birmingham
  - » Looked at top email threats over 30 days
  - » Submitted malware to virustotal.com
  - » Results:
    - Average detection rate: 25%
    - One week later, avg. detection rate: 66%
- Our experience for post-incident malware detection: 12%
- Beware of market differentiation
  - » Norton catches more than SEP, but false positive rate is higher.

KEY DEFENSE STRATEGIES

- Vulnerability and Patch
  - » Secunia
- Control of Admin Rights
  - » We do this
- Application Control
  - » Requires clients are managed – involves “trusted sources of change”
- Isolation
  - » URL Filtering
  - » Browser isolation (market not mature)

SEP TO SCEP PROJECT

- Originated as IST internal project
- Recommend for or against renewal of Symantec contract (from IST POV)
- RFP explicitly out of scope

WNAG EP SUBGROUP

- First meeting 2014-12-10
- Project/group pages at https://uwaterloo.ca/information-systems-technology/about/organizational-structure/information-security-services/examining-sep-replacements
- Still determining scope

WHAT HAS ISS-SOC BEEN DOING?

- Assumption: by the time traffic hits the endpoints, it’s already too late.
- Fact: not every infection is reported to IST.
- Result: building out network-based intrusion detection and analytics.

QUESTIONS FOR CTSC

Does campus:

- Rely on off-host protection exclusively
- Combine on-host protection with off-host
- All-in with on-host protection
- All-in on vendor “single pane of glass” type solutions

And does it need to be one size fits all?

FINAL THOUGHTS

- Endpoint Protection != Antivirus
- If something happens but it isn’t reported, what then?
- Implications of work-from-home

UNIVERSITY OF WATERLOO